IN THE CLAIMS:

Please find below a listing of all pending claims. The statuses of the claims are set forth in parentheses. For those currently amended claims, underlined emphasis indicates insertions and ~~strikethrough~~ emphasis (and/or double brackets) indicates deletions.

1. (currently amended) A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

judging whether the monitored communication has been ~~being~~ executed by the worm based on the information acquired and a predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting~~; and~~

~~changing the measurement parameters when the communication is judged to have been executed by the worm at the judging~~,

wherein the acquiring includes acquiring information of the monitored communication, based on ~~the measurement parameters changed at the changing, the~~

~~information on~~ second setting information for the plurality of setting items after the monitored communication is judged to have been executed by the worm at the judging.

2. (canceled)

3. (currently amended) A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

judging whether the monitored communication has been executed by the worm based on the information acquired and a first predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting~~; and~~

~~changing the judgment criteria when the communication is judged to have been executed by the worm at the judging~~, wherein

the judging includes further judging whether the monitored communication ~~judged to have been executed by the worm at the judging~~ has been executed by the worm after the monitored communication is judged to have been executed by the worm

at the judging, based on the information acquired and ~~the judgment criteria changed at the changing~~ a second predetermined judgment criteria.

4. (previously presented) The computer-readable recording medium according to claim 1, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.

5. (currently amended) A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

first judging whether a computer in the predetermined network segment is infected by the worm based on the information acquired and a predetermined judgment criteria;

second judging whether a plurality of computers in the predetermined network segment are infected by the worm;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged at the first judging that the computer is infected by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting, wherein

the second judging includes judging that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that

a monitored communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,

a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and

a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging.

6-7. (canceled)

8. (currently amended) A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~first setting information for a plurality of setting items;

judging whether the monitored communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged at the judging that the monitored communication is executed by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting

wherein the judging includes identifying a type of the worm executing the monitored communication by comparing features of ~~a first~~ the monitored communication with features of a ~~second~~ communication executed by a worm that are recorded in advance~~, when the first communication is judged to be executed by a worm~~.

9-12. (canceled)

13. (currently amended) A method for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

judging whether the monitored communication has been ~~being~~ executed by the worm based on the information acquired and a predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting~~; and~~

~~changing the measurement parameters when the communication is judged to have been executed by the worm at the judging~~,

wherein the acquiring includes acquiring information of the monitored communication, based on ~~the measurement parameters changed at the changing, the information on~~ second setting information for the plurality of setting items after the monitored communication is judged to have been executed by the worm at the judging.

14. (canceled)

15. (currently amended) A device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

an acquiring unit that acquires information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

a judging unit that judges whether the monitored communication has been executed by the worm based on the information acquired and a predetermined judgment criteria;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm by the judging unit; and

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit~~; and~~

~~a setting changing unit that changes the measurement parameters when the communication is judged to have been executed by the worm by the judging unit~~,

wherein

the acquiring unit acquires information of the monitored communication, based on ~~the measurement parameters changed by the setting changing unit, the information~~ on second setting information for the plurality of setting items after the monitored communication is judged to have been executed by the worm by the judging unit.

16. (currently amended) A device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

an acquiring unit that acquires information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

a judging unit that judges whether the monitored communication has been executed by the worm based on the information acquired and a first predetermined judgment criteria;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm by the judging unit; and

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit~~; and~~

~~a setting changing unit that changes the judgment criteria when the communication is judged to have been executed by the worm by the judging unit~~,

wherein

the judging unit further judges whether the monitored communication ~~judged to have been executed by the worm by the judging unit~~ has been executed by the worm after the monitored communication is judged to have been executed by the worm by the judging unit, based on the information acquired by the acquiring unit and ~~the judgment criteria changed by the setting changing unit~~ a second predetermined judgment criteria.

17. (previously presented) The device according to claim 15, wherein the judging unit judges that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.

18. (currently amended) A device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

an acquiring unit that acquires information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

a judging unit that judges at a first time whether a computer in the predetermined network segment is infected by the worm based on the information acquired and a predetermined judgment criteria, and judges at a second time whether a plurality of computers in the predetermined network segment are infected by the worm;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged at the first time by the judging unit that the computer is infected by the worm;

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit,

wherein the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that

a monitored communication from the computer in the predetermined network segment is judged at the first time to be infected by the worm,

a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the

communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm, and

a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm.

19-21. (canceled)

22. (currently amended) A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

judging whether the monitored communication has been executed by the worm based on the information acquired and a predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting,

wherein the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication ~~when the communication is judged to have been executed by the worm at the judging~~ being executed by the worm, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the monitored communication ~~judged to have been executed by the worm at the judging~~ being executed by the worm.

23. (currently amended) A method for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

judging whether the monitored communication has been executed by the worm based on the information acquired and a predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm at the judging; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting,

wherein the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication ~~when the communication is judged to have been executed by the worm at the judging~~ being executed by the worm, and extracting as the reference information, a most frequently appeared port number of the communication packets

transmitted in the monitored communication ~~judged to have been executed by the worm at the judging~~ being executed by the worm.

24. (currently amended) A device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

an acquiring unit that acquires information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

a judging unit that judges whether the monitored communication has been executed by the worm based on the information acquired and a predetermined judgment criteria;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm by the judging unit; and

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit,

wherein the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication ~~when the communication is judged to have been executed by the worm by the judging unit~~ being executed by the worm, and extracts, as the reference information, a most frequently appeared port number of the

communication packets transmitted in the monitored communication ~~judged to have been executed by the worm by the judging unit~~ being executed by the worm.

25. (currently amended) A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform a process comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

judging whether the monitored communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged at the judging that the monitored communication is executed by the worm;

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting,

wherein the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication ~~upon it being judged that the communication is executed by the worm at the judging~~ being executed by the worm, and extracting, as the reference information, a direction of the monitored

communication wherein the number of the communication packets is over a threshold value.

26. (canceled)

27. (currently amended) A method for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

judging whether the monitored communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged at the judging that the monitored communication is executed by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted at the extracting,

wherein the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication ~~upon it being judged that the communication is executed by the worm at the judging~~ being executed by the worm, and extracting, as the reference information, a direction of the monitored

communication wherein the number of the communication packets is over a threshold value.

28. (currently amended) A device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

an acquiring unit that acquires information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on ~~measurement parameters~~ first setting information for a plurality of setting items;

a judging unit that judges whether the monitored communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged by the judging unit that the monitored communication is executed by the worm;

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit,

wherein the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication ~~upon it being judged that the communication is executed by the worm by the judging unit~~ being executed by the worm, and extracts, as the reference information, a direction of the

monitored communication wherein the number of the communication packets is over a threshold value.

29-33. (canceled)

34. (currently amended) A device for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, comprising:

a worm judging unit that judges whether a monitored communication has been executed by the worm;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication judged to have been executed by the worm; and

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit,

wherein the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication ~~when the communication is judged to have been executed by the worm by the worm judging unit~~ being executed by the worm, and extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the monitored communication ~~judged to have been executed by the worm by the worm judging unit~~ being executed by the worm.

35. (currently amended) A device for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, comprising:

a worm judging unit that judges whether a monitored communication is executed by the worm;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the monitored communication upon it being judged by the worm judging unit that the monitored communication is executed by the worm; and

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit,

wherein the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication ~~upon it being judged by the worm judging unit that the communication is executed by the worm~~ being executed by the worm, and extracts, as the reference information, a direction of the monitored communication wherein the number of the communication packets is over a threshold value.

36-40. (canceled)

41. (previously presented) The computer-readable recording medium according to claim 3, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.

42. (canceled)

43. (previously presented) The computer-readable recording medium according to claim 8, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.